楕円曲線の5等分点の体について (代数的整数論)

AUTHOR(S):

広瀬, 行夫

CITATION:

広瀬, 行夫. 楕円曲線の5等分点の体について(代数的整数論). 数理解析研究所講究録 1991, 759: 180-191

ISSUE DATE:

1991-06

URL:

http://hdl.handle.net/2433/82185

数理解析研究所講究録
759巻 1991年 180-191

楕円曲線の5等分点の体について

阪大理学部　広瀬 行夫 (Yukio Hirose)

代数体K上の非可解ガロワ拡大の最も単純な例は、K-係数5次方程式の分解体すなわち S_5 (または A_5)-拡大で与えられる。一方 $\ell \neq 2,3$ を素数とするとき、K上の楕円曲線Eの ℓ 等分点により生成される体は例外を除いてK上の非可解ガロワ拡大(そこでの"相互律"はEの Hasse-Weil zeta 関数によりだいたい統制されている)であり、特にEの5等分点で生成される体は高々K上の S_5-拡大体の4次巡回拡大体となる。その S_5-拡大体を与える5次方程式を具体的に決定したのがここでの主要な結果である。

§0 結果

Kを標数0の体, EをK上の楕円曲線

$$E: Y^2 = X^3 + AX + B \quad (A, B \in K)$$

とし、j_E をEの j-invariant $(= 2^8 3^3 A^3/(4A^3+27B^2))$ とする。素数 ℓ を固定し、$E[\ell]$ をEの ℓ-torsion 元全体のなす部分群,

LはKに$E[l]$のすべての元の座標をKに付加した体（"l等分点の体"）とする。

定理　$l=5$, $j_E \neq 0, 1728$とする。Lは方程式

$$X^5+5X^4+40X^3=j_E$$

のK上の分解体の高々4次巡回拡大である。

$K=\mathbb{Q}$（有理数体）とするとき、Lは1の原始l乗根を含む事が知られているから、$L/\mathbb{Q}$でlは分岐する。lが$L/\mathbb{Q}$で wildly ramify となる基準は Serre [1] により部分的に与えられているが、$l=2,3$を除いて完全には知られていない。定理から、$l=5$の場合にだけ次の系を得た。結果はもちろん [1] と一致している。

系　$l=5$, $K=\mathbb{Q}_5$（5-進体）, $j_E \neq 0, 1728$とし、整数m, nはそれぞれj_E, j_E-1728の5の order とする。このとき$L/\mathbb{Q}_5$が wildly ramify とならない必要十分条件は、次のいずれかが成立する事である。

i)　$m \geq 2$　　ii)　$n \geq 3$

iii)　$m=n=0$　かつ　$j_E \equiv 7, 14, 21 \mod 25$

iv)　$5 \mid m < 0$　かつ　$5^{-m} j_E \equiv \pm 1, \pm 7 \mod 25$

以下、定理の証明は§2で、系の証明は§3で行う。

記号　$\bar{K}$ は K の代数閉包、ガロワ拡大 F/K に対し $G(F/K)$ でそのガロワ群をあらわす。$\mathbb{F}_\ell$, $GL_2(\mathbb{F}_\ell)$ はそれぞれ位数 ℓ の有限体と $\mathbb{F}_\ell$ 上の $(2,2)$ 型行列群をあらわす。$GL_2^+(\mathbb{F}_\ell)$, $SL_2(\mathbb{F}_\ell)$ はそれぞれ 行列式 $\in \mathbb{F}_\ell^\times$, 行列式 $=1$ なる元全体のなす $GL_2(\mathbb{F}_\ell)$ の部分群とする。自然数 n に対し、S_n は n 次対称群とする。

§1　L/K の部分体

$E[\ell]$ は $G(\bar{K}/K)$ の作用で固定されるから、L/K はガロワ拡大で $G(L/K)$ の $E[\ell]$ への作用の表現

$$\rho : G(L/K) \longrightarrow Aut\,(E[\ell])$$

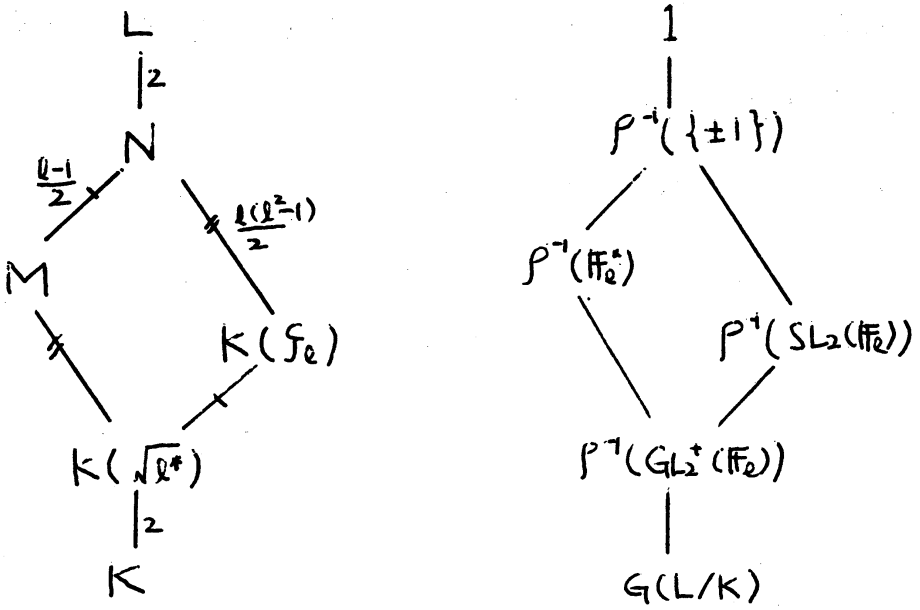
が得られる。ρ は単射である。$E[\ell]$ は加群として $\mathbb{F}_\ell \oplus \mathbb{F}_\ell$ に同型であり、その $\mathbb{F}_\ell$-basis を定めることにより $Aut\,(E[\ell])$ と $GL_2(\mathbb{F}_\ell)$ を同一視する。M, N をそれぞれ $G(L/K)$ の部分群 $\rho^{-1}(\mathbb{F}_\ell^\times)$, $\rho^{-1}(\pm 1)$ に対応する L/K の部分体とする。$\mathbb{F}_\ell^\times$ は $GL_2(\mathbb{F}_\ell)$ の center だから、M/K, N/K はガロワ拡大である。次の事実が知られている。(cf. [2] "Weil-pairing")

i) L は 1 の ℓ 乗根 ζ_ℓ を含む

ii) $\forall \sigma \in G(L/K)$ に対し、$\zeta_\ell^\sigma = \zeta_\ell^{\det \rho(\sigma)}$

よって、L/K の部分体と $G(L/K)$ の部分群の間に次の対応が

つく。（指数は $\ell \neq 2$ かつ ρ が全射のとき）



ここに、$\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$（ただし、$\ell=2$ のとき $\ell^*=1$）。

<u>G(M/K)の置換表現</u> $E[\ell]$ には $\ell+1$ 個の位数 ℓ の部分群

$$\mathcal{B} = \{B_1, \cdots, B_{\ell+1}\}$$

が含まれており、$G(L/K)$ が $\mathcal{B}$ に作用するが、この作用は ρ を通して $Aut(E[\ell]) = GL_2(\mathbb{F}_\ell)$ の $\mathcal{B}$ への作用に拡張される。$GL_2(\mathbb{F}_\ell)$ の $\mathcal{B}$ への作用の表現を

$$\varphi : GL_2(\mathbb{F}_\ell) \longrightarrow Aut(\mathcal{B}) \simeq S_{\ell+1}$$

とおくと、$\ker\varphi = \mathbb{F}_\ell^\times$ で、ρ, φ から 単射準同型

$$G(M/K) \xhookrightarrow{\rho} PGL_2(\mathbb{F}_\ell) \xhookrightarrow{\varphi} S_{\ell+1}$$

が induce される。$\ell=2,3$ を除けば、φ は全射でない。$\ell=5$ のとき、$PGL_2(\mathbb{F}_5) \simeq S_5$ が群論の一般論から知られているので、M/K は高々 S_5-拡大である。

命題1　$j_E \neq 0, 1728$ とする。K' を K の部分体、E' を K' 上の楕円曲線とし、E から M, N を定義したのと同様に E' に対し M', N' を定義する。このとき

$$j_E = j_{E'} \Rightarrow M = kM',\ N = kN'$$

証明は、$j_E = j_{E'}$ から E と E' が K 上同型なる事と、$j_E \neq 0, 1728$ から $Aut(E), Aut(E') = \{\pm 1\}$ なる事から容易に従う。

§2　定理の証明

以下 $l = 5$, $j_E \neq 0, 1728$ とする。M の定義方程式が定理の方程式なる事を示せばよい。命題1により定理の証明のためには、K, E を次の形

$$K = \mathbb{Q}(c) \quad (c \neq 0, 1)$$

$$E = E_c : y^2 = x^3 - 3cx - 2c \quad \left(c = \frac{j_E}{j_E - 1728}\right)$$

に制限して十分である。次の補題が基本的である。

補題　Λ を index の集合の集合

$$\Lambda = \left\{ \{\{i,j\}, \{k,l\}, \{m,n\}\} \mid \{i,j,k,l,m,n\} = \{1,2,\cdots,6\} \right\}$$

とおく。$|\Lambda| = 15$ で、S_6 を Λ に対し自然に作用させる。このとき、§1 の φ を通して得られる $PGL_2(\mathbb{F}_5)$ の Λ への作用に関し、次が成立する。

1) Λ の推移域分解は

$$\Lambda = \Lambda_1 \cup \Lambda_2 \ ; \ |\Lambda_1| = 5 \ , \ |\Lambda_2| = 10$$

$$, \ \Lambda_1 = \{\{\{i,j\},\{k,l\},\{m,n\}\} \in \Lambda \mid (i\,j)(k\,l)(m\,n) \notin \varphi(PGL_2(\mathbb{F}_5))\}$$

2) $PGL_2(\mathbb{F}_5)$ の Λ_1 への作用は faithful すなわち.

$$PGL_2(\mathbb{F}_5) \hookrightarrow Aut\,\Lambda_1 \cong S_5$$

証明 補題の証明は計算機で行われた。■

今、各 $i = 1, \cdots, 6$ に対し、

$$w_i \overset{def}{=} \frac{1}{4} \sum_{0 \neq P \in B_i} x(P) \qquad (x(P) \text{ は } P \text{ の } x \text{ 座標})$$

各 $\lambda = \{\{i,j\},\{k,l\},\{m,n\}\} \in \Lambda$ に対し、

$$u_\lambda \overset{def}{=} w_i w_j + w_k w_l + w_m w_n$$

と定める。明らかに $w_i \in M$ で $\sigma \in G(L/k)$ に対し $\sigma(B_i) = \sigma(B_j)$ ならば $\sigma(w_i) = w_j$, $(\varphi \circ \rho(\sigma))(i) = j$ である。よって補題の 1) により

$$h(X) \overset{def}{=} \prod_{\lambda \in \Lambda_1} (X - u_\lambda)$$

は k-係数 5 次多項式で、補題の 2) により u_λ; $\lambda \in \Lambda_1$ がたいに異なる限りにおいて、$h(X)$ は M を定義する多項式である。ところで、C を不定元にとれば、15 次多項式 $H(X) \overset{def}{=} \prod_{\lambda \in \Lambda} (X - u_\lambda)$ は次節にのべる方法により、X と C の $\mathbb{Q}$-係数多項式として実際に具体的に計算される。そこで、$H(X)$

が具体的にわかったものとして、話を進める。$H(x)$ は実際に、5次と10次の多項式に $\mathbb{Q}(c)[x]$ で因数分解され、それらは c が不定元なる限り $\mathbb{Q}(c)$ 上既約である。5次の成分の方を仮に（x との多項式である意味も込めて）$h_1(x,c)$ とかけば、c が $\mathbb{Q}$ 上超越的ならば明らかに $h_1(c,x)$ は $h(x)$ と一致する。又、c が $\mathbb{Q}$ 上代数的であっても、c に収束する $\mathbb{C}-\overline{\mathbb{Q}}$（$\mathbb{C}$ は複素数体）の数列 $\{c_n\}$ をとるとき、$\exists c_n$ に対し定義される $h(x)$ $(=h_1(c_n,x))$ が $\exists c$ に対し定義される $h(x)$ に（係数ごとに）収束するのは明らかなので、この場合も $h(x)=h_1(c,x)$ を得る。適当な x の $\mathbb{Q}(c)$ 上の一次分数変換により、$h_1(c,x)$ は定理の方程式に変形される。又、定理の方程式の判別式は（すべての $\lambda \neq 0, 1728$ に対し）0 でない事も容易に確かめられるから、$\{u_\lambda ; \lambda \in \Lambda_1\}$ は互いに異なる。よって定理の方程式の K 上の分解体は M である。∎

<u>$H(x)$ の計算</u>　計算結果は繁雑なので、ここでは計算手順のみを述べる。実行は計算機による数式処理で行われた。計算は次の3段階に分けられる。1）"5等分多項式" の計算　2）$g(x) \overset{\text{def}}{=} \prod_{i=1}^{6}(x-w_i)$ の計算　3）$H(x)$ の計算

1）<u>"5等分多項式"</u>　$P, Q \in E$ に対し、$x(P)=x(Q)$ $\Leftrightarrow P=\pm Q$ だから

$f(X) \overset{\text{def}}{=} \prod (X - x)$; $x \in \{ x(P)$; $O \neq P \in E[5] \}$

は k-係数 12 次の多項式で、その分解体は N である。これを 5等分多項式と呼ぶ。E の加法公式から、$P = (x, y) \in E$ に対し

$$x(2P) = \frac{x^4 + 6Cx^2 + 16Cx + 9}{4y^2} \qquad (\to -32C^2 + 27C^3)$$

$$x(3P) = x - \frac{8y^2(x^6 - 15Cx^4 - 40Cx^3 - 45C^2x^2 - 24C^2x}{(3x^4 - 18Cx^2 - 24Cx - 9C^2)^2}$$

である。$x(2P) = x(3P)$ $(\Leftrightarrow P \in E[5])$ とおいて、y^2 に $x^3 - 3Cx - 2C$ を代入すれば $f(X)$ を得る。

2) $g(X)$ の計算　$1 \leq \forall i \leq 6$, $O \neq \forall P \in B_i$ に対し、

$$w_i = \frac{1}{2}(x(P) + x(2P)) = a(x(P)) / b(x(P))$$

ここに、$a(X) = 5X^4 - 6CX^2 + 8CX + 9C^2$

$b(X) = 8(X^3 - 3CX - 2C)$

となる事が容易に確かめられる。$b(X) = 0$ の根は E の2等分点の x 座標であるから、$b(X)$ と $f(X)$ は $k[X]$ で互いに素である。よって互除法を用いて、$b(X)t(X) \equiv 1 \mod f(X)$ なる $t(X) \in k[X]$ が求まる。$w(X) = a(X)t(X)$ とおいて、$m = 1, \cdots, 6$ に対し、$w(X)^m$ を $f(X) = 0$ で環元する事により、$W_m(X) \equiv w(X)^m \mod f(X)$, $\deg W_m(X) \leq 11$ なる $W_m(X) \in k[X]$ が求まる。しからば $1 \leq \forall i \leq 6$, $O \neq \forall P \in B_i$ に対し、

$$w_i^m = W_m(x(P))$$

である。今、任意の多項式 $F(X) \in k[X]$ と $m \in \mathbb{Z}$ に対し、

$$[m]_F \overset{\text{def}}{=} \Sigma_{F(x)=0} x^m$$

と定める。Newton の公式を用いれば $g(x)$ を求めるためには、$[m]_g$; $m=1,\cdots,6$ を $[\ ]_f$ であらわす事を考えればよい。$W_m(x) = \Sigma_{j=0}^{11} a_j^{(m)} X^j$ とおけば

$$[m]_g = \Sigma_{i=1}^{6} w_i^m = \Sigma_{i=1}^{6} \left(\frac{1}{4} \Sigma_{0 \neq p \in B_i} W_m(\chi(p)) \right)$$
$$= \frac{1}{2} \Sigma_{f(x)=0} W_m(x) = \frac{1}{2} \Sigma_{j=0}^{11} a_j^{(m)} [j]_f$$

(以上の方法により、
$g(x) = X^6 - C(15X^4 + 40X^3 + 45CX^2 + 24CX + 5C)$.)

3) $H(x)$ の計算　常識的には $H(x)$ を $w_1, \cdots, w_6, X$ の多項式に展開して X^m の係数を $w_1, \cdots, w_6$ の基本対称式であらわす事をやればよいのだが それでは計算があまりにぼう大となるので 2) と同様 $[\ ]_H$ を $[\ ]_f$ であらわす事を考える。そのためには、更に次の公式が必要である。

(公式) 多項式 $F(x) = \Pi_{i=1}^{n} (X - \lambda_i)$ に対し、$[\ ,\cdots,\ ]_F$ を漸化式
$$[k_1, \cdots, k_d, k]_F \overset{\text{def}}{=} [k_1, \cdots, k_d]_F [k]_F - \Sigma_{i=1}^{n} [k_1, \cdots, k_{i-1}, k_i + k, k_{i+1}, \cdots, k_d]_F$$
により定める。このとき $1 \leq \forall d \leq n$ に対し
$$\Sigma_{\sigma \in S_n} \lambda_{\sigma(1)}^{k_1} \cdots \lambda_{\sigma(n)}^{k_d} = (n-d)! [k_1, \cdots, k_n]_F$$

証明は帰納法によれば容易なので省略する。公式を用いて $[m]_H$ は次の様に計算される。

$$[m]_H = \Sigma_{\lambda=1}^{15} u_\lambda^m = \frac{15}{|S_6|} \Sigma_{\sigma \in S_6} (w_{\sigma(1)} w_{\sigma(2)} + w_{\sigma(3)} w_{\sigma(4)} + w_{\sigma(5)} w_{\sigma(6)})^m$$

$$= \frac{1}{48} \sum_{\substack{p+q+r=m \\ p,q,r\geq 0}} \frac{m!}{p!q!r!} \sum_{\sigma} w_{\sigma(1)}^{p} w_{\sigma(2)}^{p} w_{\sigma(3)}^{q} w_{\sigma(4)}^{q} w_{\sigma(5)}^{r} w_{\sigma(6)}^{r}$$

$$= \frac{m!}{24} \sum_{p,q,r} \frac{g(0)^r}{p!q!r!} [p-r, p-r, q-r, q-r]_g$$

$[p-r, p-r, q-r, q-r]_g$ は $[p-r]_g$, $[2q-2r]_g$ 等々であらわされ、$[m]_H$ を $[\ ]_g$ から計算する事ができる。

§3 系の証明

次の4つの場合：1) $m>0$, 2) $n>0$, 3) $m=n=0$, 4) $m=n<0$ に分けて、下の命題2を $p=5$, $k=\mathbb{Q}_5$, $F(X)=X^5+5X^4+40X^3-d_E$ において適用すれば容易に証明される。■

命題2 pを素数，kをp-進体$\mathbb{Q}_p$の有限次拡大体，vをkの指数付値で$v(k^\times)=\mathbb{Z}$とする。$F(X)$をk-係数，p次，monicなる多項式でその判別式$disc\,F\neq 0$とする。Ωを$F(X)$のk上の分解体とするとき、下の手順(0)～(3)を有限回ループする事により

(*) Ω/k は wildly ramify

になるか否かを判別できる。

(0) a_i $(i=1,\cdots,p)$ を $F(X)$ の X^{p-i} の係数，$N=v(a_p)$ と定める．

(1) $1\leqq i\leqq p-1$ s.t. $v(a_i)\leqq \frac{i}{p}n$ ならば(*)でない。

その他の場合,

(2) $p \nmid N$ ならば (*) である。

その他の場合,

(3) $v(x^p + a_p) > N$ なる $x \in k$ がとれ, $F(x)$ を $F(X+x)$ におきかえて (0) へ戻る。

<u>証明</u> π を k の素元、また v は Ω 上まで拡張しておく。まず手順の名段階の正当性を示す。

(1) の正当性: (*) であるとする ($1 \leqq \forall i \leqq p-1, v(a_i) > \frac{i}{p}N$ を示す)。$F(X)$ は k 上既約となり、$F(X)$ の任意の根 α に対し $v(\alpha) = \frac{N}{p}$。故に $1 \leqq \forall i \leqq p$, $v(a_i) \geqq \frac{i}{p}N$. よって $p \nmid N$ ならば $1 \leqq \forall i \leqq p-1$, $v(a_i) > \frac{i}{p}N$. $p \mid N$ とする。$G(X) = F(\pi^{\frac{N}{p}}X)/\pi^N$ は整係数, monic でその根 β は Ω の整数。$k(\beta)/k$ は totally ramify すなわち residue class degree は 1。よって k の整数 r が存在して $v(\beta - r) > 0$ 共役をとれば $G(X)$ の他の根 β' に対しても $v(\beta' - r) > 0$ となる。よって $G(X) \equiv X^p - r^p \bmod \pi$ すなわち $1 \leqq \forall i \leqq p-1$, $v(a_i) > \frac{i}{p}N$ である。

(2) の正当性: $v(a_i) > \frac{i}{p}N$ $(i = 1, \cdots, p-1)$, $p \nmid n$ として (*) を示す。$F(X)$ の Newton polygone をみれば $F(X)$ は k 上既約がわかり, $F(X)$ の根 α に対し $v(\alpha) = \frac{N}{p}$。よって (*) である。

(3)の正当性：$p \mid N$ なるとき $v(x^p + a_p) > N$ なる $x \in k$ は $y^p \equiv a_p/\pi^N$ なる y をとって $x = \pi^{\frac{N}{p}} y$ とおけばとれる。

(0)～(3) のループが有限回で止まることの証明：(3)の時点において考えると、$p \mid N$ で、$1 \leqq \forall i \leqq p-1$ に対し、$v(a_i) > \frac{i}{p}N$ である。よって $G(X) = F(\pi^{\frac{N}{p}}X)/\pi^N$ は整係数，monic で，$0 \leqq v(\mathrm{disc}\, G) = v(\mathrm{disc}\, F) - N(p-1)$ すなわち，$N \leqq v(\mathrm{disc}\, F)/(p-1)$ $(< \infty)$。一方，$v(x^p + a_p) > N$ より $v(F(x)) > N$ となり，次回のループにおいて N は増大している。$v(\mathrm{disc}\, F)$ はループを重ねる度に不変であるから，ループは有限回で止まらねばならない。∎

文献

[1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. 15 (1972), 259-331

[2] J. H. Silverman "The Arithmetic of elliptic curves," Graduate texts in mathematics 106, Springer-Verlag